07 Juin 2021

Lettre ouverte appelant à l'interdiction mondiale du recours à la reconnaissance faciale et à la reconnaissance biométrique à distance permettant une surveillance de masse et une surveillance ciblée discriminatoire

Nous, les soussigné·e·s, demandons l'interdiction totale du recours aux technologies de reconnaissance faciale et de reconnaissance biométrique à distance qui permettent une surveillance de masse et une surveillance ciblée discriminatoire. Ces outils ont la capacité d'identifier, de suivre, de distinguer et de repérer des personnes où qu'elles aillent, compromettant ainsi nos droits fondamentaux et nos libertés civiles - notamment les droits à la vie privée et à la protection des données, le droit à la liberté d'expression, le droit à la libre association (ce qui mène à la criminalisation des actions de protestation et a un effet dissuasif), et les droits à l'égalité et à la non-discrimination.

Nous avons constaté que les technologies de reconnaissance faciale et de reconnaissance biométrique à distance sont utilisées dans le but de rendre possible une longue liste de violations des droits humains. En Chine, aux États-Unis, en Russie, en Angleterre, en Ouganda, au Kenya, en Slovénie, au Myanmar, aux Émirats arabes unis, en Israël et en Inde, la surveillance visant manifestant·e·s et civil·e·s a compromis le droit de personnes à la vie privée et le droit à la libre association. Les arrestations injustifiées de personnes innocentes aux États-Unis, en Argentine et au Brésil ont porté atteinte au droit de ces personnes à la vie privée, au droit à un procès équitable et au droit de circuler librement. La surveillance de membres de minorités ethniques et religieuses, ainsi que d'autres populations marginalisées et opprimées en Chine, en Thaïlande et en Italie a bafoué le droit de ces personnes à la vie privée et leur droit à l'égalité et à la non-discrimination.

Ces technologies menacent délibérément les droits des citoyen·ne·s et ont déjà causé de graves préjudices. Aucune mesure de protection technique ou juridique ne pourrait totalement éradiquer le risque qu'elles représentent, et nous pensons donc qu'elles ne doivent jamais être utilisées en public ni dans des espaces accessibles au public, que ce soit par des gouvernements ou par le secteur privé. Le risque d'abus est trop grand, et les conséquences trop graves.

Nous demandons une interdiction parce que même si un moratoire permettait de suspendre temporairement le développement et l'utilisation de ces technologies, et de gagner du temps afin de recueillir des éléments de preuve et d'organiser un débat démocratique, il est déjà manifeste que ces enquêtes et discussions ne feront que confirmer que **le recours à ces technologies dans des espaces**

accessibles au public est incompatible avec nos droits fondamentaux et libertés civiles, et doit être totalement et définitivement interdit.

La portée de notre appel

Les termes « reconnaissance faciale » et « reconnaissance biométrique à distance » couvrent un vaste ensemble de technologies, du système de reconnaissance faciale qui déverrouille le téléphone d'une personne, ou autorise l'accès à certains espaces, à la technologie identifiant la démarche d'une personne, en passant par les systèmes prétendant détecter l'identité de genre ou l'état émotionnel.

Notre appel à l'interdiction porte spécifiquement, sans toutefois y être limité, au recours à ces technologies afin d'identifier ou de distinguer une personne dans un large groupe d'individus, soit le fait de procéder à une reconnaissance faciale ou biométrique (comparaison un-à-plusieurs). Nous déplorons que ces technologies soient utilisées afin d'identifier, de distinguer, ou de suivre à la trace des personnes en utilisant leur visage, leur démarche, leur voix, leur apparence personnelle, ou toute autre donnée biométrique d'une manière qui permette une surveillance de masse ou une surveillance ciblée discriminatoire, comme par exemple une surveillance ayant un impact disproportionné sur les droits fondamentaux et les libertés civiles de minorités religieuses, ethniques et raciales, d'opposant·e·s politiques, et d'autres groupes marginalisés. Nous savons également que, dans certains cas, les systèmes de reconnaissance biométrique, notamment faciale (par exemple, la comparaison un-à-plusieurs), peuvent être conçus et utilisés d'une manière qui donne lieu à des formes de surveillance problématiques, notamment en créant de larges bases de données centralisées pouvant être réutilisées à d'autres fins.

Si certaines applications de reconnaissance faciale et de reconnaissance biométrique à distance prétendent protéger la vie privée des personnes en n'établissant pas de lien avec leur identité juridique, elles peuvent toutefois être utilisées pour repérer certains individus dans les espaces publics, ou pour tirer des conclusions quant à leurs caractéristiques et leur comportement. Dans toutes ces situations, peu importe que les données soient rendues anonymes afin de protéger les informations qui permettraient d'identifier des personnes ou soient uniquement traitées localement (par exemple sur un réseau de périmètre) ; nos droits sont compromis quoi qu'il arrive parce que ces outils sont essentiellement conçus pour rendre possible et autoriser la surveillance des personnes d'une manière qui est incompatible avec nos droits.

Par ailleurs, de nombreuses applications de classification faciale et biométrique, qui font des déductions et des prédictions sur des éléments tels que le genre, les émotions ou d'autres attributs personnels, présentent de graves lacunes sur le plan scientifique. Cela signifie que leurs déductions sont souvent incorrectes, et dans certains cas s'appuient même sur les théories eugénistes de la phrénologie et de la physiognomonie, perpétuant ainsi des discriminations et aggravant les choses puisque nous sommes à la fois surveillés et présentés sous un faux jour.

Notre appel en faveur d'une interdiction concerne le recours à ces technologies lorsqu'elles sont utilisées à des fins de surveillance dans des espaces accessibles au public et dans des espaces que les gens ne peuvent éviter de fréquenter. Si l'emploi de ces technologies par les organes responsables de l'application des lois attire l'attention et suscite des critiques, leur utilisation par des acteurs privés peut menacer nos droits de la même façon, en particulier lorsque ces acteurs privés mènent une surveillance pour le compte de gouvernements et d'institutions publiques dans le cadre de partenariats public-privé, ou fournissent aux autorités des informations provenant de cette surveillance.

Nous avons aussi pu observer une évolution inquiétante, selon laquelle des fournisseurs privés de services de reconnaissance faciale compilent et fusionnent des bases de données d'individus « suspects », et partagent ces données avec divers clients. Cela crée dans les faits des « bases de données nationales » mises en commun avec d'autres entreprises privées, qui sont compilées à la discrétion de personnels non formés, ne sont soumises à aucune supervision, et qui sont susceptibles de mener à des discriminations contre les personnes apparaissant sur des listes de surveillance dans tous les lieux où ces bases de données sont utilisées.

Le recours à ces technologies pour surveiller les gens dans les parcs, les écoles, les bibliothèques, au travail, dans les réseaux de transport, les stades, les ensembles d'habitat, et même en ligne, notamment sur les réseaux sociaux, constitue une menace existentielle à nos droits fondamentaux et libertés civiles, et ces pratiques doivent impérativement cesser.

Pourquoi une interdiction ?

Les technologies de reconnaissance faciale et de reconnaissance biométrique à distance présentent des lacunes techniques considérables dans leur forme actuelle, notamment les systèmes de reconnaissance faciale reflétant des préjugés raciaux, qui sont moins précis pour les personnes ayant la peau sombre. Améliorer ces systèmes sur le plan technique n'éliminera cependant pas la menace qu'ils représentent pour nos droits humains et nos libertés civiles.

S'il est possible qu'ajouter des données d'apprentissage plus inclusives ou que prendre d'autres mesures afin d'améliorer la précision de ces systèmes apporte des solutions à certains des problèmes actuels, cela aura aussi pour effet de les perfectionner en tant qu'instruments de surveillance et de les rendre plus efficaces pour affaiblir nos droits.

Ces technologies menacent nos droits de deux manières principales :

Tout d'abord, les données d'apprentissage - les bases de données de visages auxquelles sont comparées les données saisies, et les données biométriques traitées par ces systèmes - sont généralement obtenues sans que l'intéressé·e ne le sache, n'y consente, ni ne puisse prendre le choix

éclairé d'y être inclus, ce qui signifie que ces technologies encouragent à dessein à la fois la surveillance de masse et la surveillance ciblée discriminatoire.

Ensuite, tant que les personnes évoluant dans des espaces accessibles au public pourront être instantanément identifiées, repérées, ou suivies à la trace, leurs droits fondamentaux et leurs libertés civiles seront compromis. Même l'idée que ces technologies puissent être opérationnelles dans des espaces accessibles au public a un effet dissuasif qui porte atteinte à la capacité des personnes à exercer leurs droits.

Malgré des affirmations contestables selon lesquelles ces technologies améliorent la sécurité publique, la violation systématique de nos droits l'emportera toujours largement sur les éventuels avantages. Un nombre croissant d'éléments de preuve attestent que ces technologies sont utilisées à mauvais escient et déployées d'une manière qui n'est pas transparente ou si peu.

Toute enquête ou analyse portant sur la manière dont le maintien de l'ordre a historiquement été effectué montre que l'utilisation expérimentale de technologies de surveillance incrimine souvent les populations à faibles revenus et marginalisées, notamment les populations de couleur, soit les mêmes personnes qui sont généralement les victimes du racisme structurel et de discriminations. Le recours aux technologies de reconnaissance faciale et de reconnaissance biométrique à distance ne fait pas exception à cela, et c'est pour cette raison qu'il faut y renoncer avant qu'une infrastructure de surveillance encore plus dangereuse ne soit créée ou ne devienne permanente.

La simple existence de ces outils, qu'ils soient entre les mains des organes chargés de l'application des lois ou d'entreprises privées (ou dans le cadre de partenariats public-privé), favorisera toujours les détournements d'usage et la surveillance accrue des espaces publics, ce qui a un effet dissuasif sur la libre expression. Si leur existence fragilise en soi nos droits, et s'il est impossible de superviser efficacement ces technologies d'une manière qui prévienne les abus, il n'y a pas d'autre solution que d'interdire complètement leur utilisation dans les espaces accessibles au public.

À quoi ressemblera une interdiction ?

Certaines technologies de surveillance sont tout simplement si dangereuses qu'elles causent inévitablement beaucoup plus de problèmes qu'elles n'en règlent. Avec les technologies de reconnaissance faciale et de reconnaissance biométrique à distance qui permettent une surveillance de masse et une surveillance ciblée discriminatoire, le risque d'abus est trop grand, et les conséquences trop graves.

Il n'y a pas de place pour le doute : la protection des droits fondamentaux et des libertés civiles exige l'interdiction de l'utilisation de ces technologies dans les espaces accessibles au public, par les autorités au niveau des pays, des États, des provinces, des municipalités et autres, à tous les échelons, et en particulier les organes chargés de l'application des lois et du contrôle des frontières, qui disposent déjà de ressources humaines et technologiques suffisantes pour maintenir la sécurité.

07 Juin 2021

En tant que réseau mondial d'organisations de la société civile, nous reconnaissons que chaque pays a différentes manières d'élaborer des solutions mettant en avant les droits humains, dans des systèmes constitutionnels, conventionnels ou juridiques dont chacun est unique.

Quels que soient les moyens employés, le résultat doit toutefois être l'interdiction complète de l'utilisation de ces technologies dans le but de surveiller, identifier, repérer, classifier et suivre des personnes dans les espaces accessibles au public.

C'est pour ces raisons que nous exhortons :

1.) **les décideurs politiques et législateurs à tous les échelons**, dans le monde entier, à :

   a. suspendre les investissements publics dans les modes d'utilisation des technologies de reconnaissance faciale et de reconnaissance biométrique à distance qui permettent la surveillance de masse et la surveillance ciblée discriminatoire ;

   b. adopter des lois, statuts et/ou réglementations exhaustifs qui :

      i. interdisent le recours à ces technologies pour la surveillance du public et des espaces accessibles au public, notamment les transports publics, par les autorités ou en leur nom, au niveau national, fédéral, des États, des provinces, des municipalités, et/ou d'autres subdivisions politiques, y compris par leurs organes, services, secrétariats, ministères, bureaux exécutifs, conseils, commissions, ou des intervenants extérieurs, et/ou d'autres subdivisions ; en mettant particulièrement l'accent sur tous les types d'organes chargés de l'application des lois, du contrôle des frontières et du renseignement ;
      ii. prohibent l'utilisation de ces technologies par des entités privées dans les espaces publics, les espaces accessibles au public et les lieux d'accueil du public où ce type d'utilisation pourrait donner lieu à une surveillance de masse ou une surveillance discriminatoire ciblée, notamment, mais pas exclusivement, leur utilisation dans les parcs, les écoles, les bibliothèques, les lieux de travail, les réseaux de transports, les stades et les ensembles d'habitat ;
      iii. interdisent aux organes gouvernementaux, notamment ceux qui sont chargés de l'application des lois, d'obtenir et d'utiliser des données et informations tirées du recours à ces technologies par des entreprises et d'autres acteurs privés, sauf à des fins de vérification ou de contrôles de conformité ;
      iv. protègent les personnes contre la possibilité que ces technologies soient utilisées dans la prise de décisions liées aux droits économiques, sociaux et culturels, notamment le logement, l'emploi, les prestations sociales et les soins de santé ;

v. excluent le recours à ces technologies, et aux informations obtenues au moyen de celles-ci, à titre de preuve afin de poursuivre en justice ou accuser des personnes dans l'objectif de les emprisonner ou de les soumettre à une autre forme de privation de liberté ; et
vi. restreignent l'accès gouvernemental aux informations biométriques stockées par des entreprises privées ;

c. établir des règles et réglementations interdisant l'acquisition de ces technologies par des gouvernements et des organes gouvernementaux pour des utilisations permettant la surveillance de masse et la surveillance ciblée discriminatoire ;

d. cesser d'utiliser les technologies de reconnaissance faciale et biométrique à distance pour une surveillance de masse ou une surveillance ciblée discriminatoire visant des minorités religieuses, ethniques et raciales, ou des opposant·e·s politiques et d'autres groupes marginalisés ;

e. réclamer la divulgation du recours à ces technologies aux personnes en ayant fait l'objet à leur insu et n'ayant pas eu la possibilité d'exercer leurs droits au respect d'une procédure régulière pour contester l'utilisation de ces technologies ; et

f. offrir des réparations adéquates aux personnes ayant subi un préjudice du fait de l'utilisation de ces technologies ;

2.) **les tribunaux et agents du système judiciaire** à reconnaître les menaces existentielles aux droits humains découlant du recours à ces technologies et à faire le nécessaire afin de prévenir, et si besoin est, de réparer les torts causés par leur utilisation ; et

---

3.) **les organismes administratifs**, notamment les instances chargées de la protection des données et de la protection des consommateurs, à user pleinement de leur autorité afin de protéger la vie privée et les droits des consommateurs, notamment en demandant aux entreprises de cesser d'utiliser ces technologies.

Enfin, nous reconnaissons que la menace existentielle représentée par les technologies de reconnaissance faciale et de reconnaissance biométrique à distance doit être combattue non seulement par les pays et les institutions de toute sorte, mais également par d'autres acteurs importants au niveau international et national.

C'est pour cette raison que nous demandons aux :

1.) **Organisations internationales telles que le Haut-Commissariat aux droits de l'homme des Nations unies**, de passer à la vitesse supérieure et de condamner le développement et l'utilisation actuels des technologies de reconnaissance faciale et de reconnaissance biométrique à distance dans le but de surveiller certaines populations à travers le monde ;

2.) **Entités privées** qui conçoivent ou utilisent des technologies de reconnaissance faciale ou de reconnaissance biométrique à distance de :

a. s'engager publiquement à cesser la création, le développement, la vente et l'utilisation de technologies de reconnaissance faciale ou de reconnaissance biométrique à distance permettant une surveillance de masse ou une surveillance ciblée discriminatoire ;
b. cesser immédiatement la production de technologies de reconnaissance faciale ou de reconnaissance biométrique à distance permettant la surveillance de masse et la surveillance ciblée discriminatoire, et de supprimer toutes les données biométriques acquises de manière illégitime utilisées pour concevoir des bases de données, et tous les autres modèles ou produits s'appuyant sur ces données ;
c. diffuser des rapports de transparence fournissant des détails sur tous leurs contrats publics (qu'ils soient suspendus, en cours ou en projet) pour la livraison de ces technologies ; et
d. établir un dialogue véritable et s'abstenir de sanctionner les employé·e·s s'organisant sur leur lieu de travail afin de contester ou de refuser le développement des technologies de reconnaissance faciale ou de reconnaissance biométrique à distance qui permettent une surveillance de masse et une surveillance ciblée discriminatoire ;

3.) **Employés d'entreprises technologiques**, avec le soutien des syndicats, de s'organiser contre le développement ou la vente des technologies de reconnaissance faciale ou de reconnaissance biométrique à distance, dans la mesure du possible ;

4.) **Investisseurs et institutions financières** de **:**

a. mener des vérifications préalables sur le terrain des droits humains concernant leurs investissements en cours et futurs dans des entreprises développant et vendant des technologies de reconnaissance faciale ou de reconnaissance biométrique à distance, afin de déterminer quand ces technologies sont incompatibles avec le respect des droits fondamentaux et permettent une surveillance de masse et une surveillance ciblée discriminatoire ; et,

b. demander aux entreprises dans lesquelles ils investissent de cesser de créer, développer, vendre ou mettre à disposition ces technologies d'une manière qui permette une surveillance de masse et une surveillance ciblée discriminatoire ;

5.) **Organisations donatrices** de garantir le financement de procédures judiciaires et d'actions de plaidoyer lancées par des organisations non gouvernementales et organisations de la société civile cherchant à obtenir des réparations devant les tribunaux et s'impliquant activement dans les décisions politiques au niveau local, des États, des provinces, national, fédéral, supranational, régional et international, et au sein des systèmes internationaux.

Conclusion

Nous demandons à la société civile, aux militant·e·s, aux intellectuel·le·s et aux autres parties intéressées dans le monde entier de signer cette lettre et de rejoindre notre combat pour que l'utilisation de ces technologies dans les espaces accessibles au public soit interdite dès maintenant et pour toujours, afin que nos droits humains et libertés civiles soient protégés.

Pour plus d'informations sur cette initiative, contactez **banBS@accessnow.org**. Vous pouvez apporter votre soutien et consulter la liste complète des signataires sur la page: **accessnow.org/ban-biometric-surveillance**

Cette lettre ouverte a été rédigée par Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF), et l'Instituto Brasileiro de Defesa do Consumidor (IDEC).