



STOP
RECONNAISSANCE FACIALE

Papier de position

Interdiction de l'utilisation de systèmes de reconnaissance biométrique dans les espaces accessibles au public

Contexte

Que sont les systèmes de reconnaissance biométrique ?

D'une part, les systèmes de reconnaissance biométrique sont utilisés pour *authentifier* des individus (one-to-one matching). La vérification des données biométriques, telle qu'elle est utilisée pour le contrôle des frontières à l'aéroport de Zurich, en est un exemple. Pour ce faire, on ne recourt pas nécessairement à une base de données, on compare par exemple le document d'identité d'une personne avec son visage et on le soumet à une vérification.

D'autre part, les systèmes de reconnaissance biométrique sont également employés pour identifier un individu à partir d'une foule (one-to-many matching), en ayant recours à une base de données biométriques. Les explications qui suivent se réfèrent à ce deuxième type d'application. Une forme de système de reconnaissance biométrique de plus en plus utilisée est **la reconnaissance faciale**. Toutefois, il existe également des systèmes permettant d'identifier des personnes à partir de leur démarche, de leurs yeux, de leur voix ou d'autres données biométriques.

Où sont utilisés les systèmes de reconnaissance biométrique ?

Les systèmes de reconnaissance faciale et autres systèmes biométriques sont actuellement expérimentés et utilisés à une vitesse alarmante dans toute l'Europe. On les trouve notamment dans les stades, les aéroports, les casinos et même dans les écoles. Les forces de police les utilisent à des fins de répression et, dans plusieurs pays, de tels systèmes ont également été utilisés lors de la pandémie de COVID-19 comme outils de contrôle des mesures de distanciation sociale.

En Suisse, les systèmes de reconnaissance faciale sont utilisés par certaines polices cantonales à des fins de poursuite pénale, notamment dans les cantons d'Argovie, de Neuchâtel, de Schaffhouse, de Saint-Gall et de Vaud. Cette technologie est également utilisée par des particuliers, par exemple pour contrôler le certificat Covid dans les hôtels ou pour réguler l'accès des membres des salles de sport.

Un défi particulier réside dans le fait qu'il n'existe en principe que peu de transparence sur les lieux et les personnes qui utilisent des systèmes de reconnaissance biométrique. Cela constitue un obstacle de taille qui empêche un débat public factuel sur le sujet.

stop-reconnaissancefaciale.ch

Une alliance de :
AlgorithmWatch Suisse
Amnesty International Suisse
Société Numérique Suisse

Papier de position
Page 1 sur 8



STOP RECONNAISSANCE FACIALE

Situation juridique initiale

Dans la loi suisse révisée sur la protection des données (nLPD) qui entrera en vigueur en 2023, les données biométriques sont considérées comme sensibles dans la mesure où elles identifient clairement une personne physique. **Le traitement de telles données - par exemple par des systèmes de reconnaissance biométrique - n'est pas autorisé de manière générale** : une base légale (définie formellement dans une loi) est nécessaire pour leur utilisation. **Parallèlement, il n'existe pas non plus d'interdiction explicite de leur utilisation.** Il serait donc en principe possible de mettre en place des bases légales autorisant le traitement de données personnelles sensibles.

La nLPD ne s'applique qu'aux autorités fédérales et aux acteurs privés. Les cantons ne sont donc pas concernés par cette loi. Toutefois, une base légale suffisante est également nécessaire pour l'utilisation de systèmes de reconnaissance biométrique par les autorités cantonales. Bien que la question de savoir si les bases légales existantes sont suffisantes soit controversée, **certains cantons utilisent déjà des systèmes de reconnaissance faciale dans le cadre de leurs procédures pénales.** Des juristes de renom sont d'avis qu'une telle base **n'existe pas** et que l'utilisation de ces systèmes est donc illégale.

Le traitement de données sensibles requiert une base légale inscrite formellement dans une loi car le traitement de telles données par des systèmes de reconnaissance biométrique est considéré comme **une grave atteinte au droit à l'autodétermination en matière de données personnelles** (art. 13, al. 2, Cst.). En outre, une telle atteinte aux droits fondamentaux par les autorités fédérales ou cantonales ne peut être justifiée que si elle repose sur une base légale, si elle est proportionnée, si elle est justifiée par un intérêt public suffisant et si elle ne porte pas atteinte à l'essence des droits fondamentaux (art. 36 Cst.).

Depuis le début de la campagne "Stop à la reconnaissance faciale", **plusieurs interventions politiques ont été déposées au niveau communal et cantonal** pour demander l'interdiction des systèmes de reconnaissance biométriques dans les lieux accessibles au public :

- Conseil communal Zurich: [Postulat 2021/451](#) et [Motion 2021/450](#)
- Conseil communal Lausanne: [Projet de règlement](#); [Projet de règlement](#), [Postulat](#)
- Grand Conseil de Bâle-Ville : [Anzug 22.5022](#)



STOP RECONNAISSANCE FACIALE

Pourquoi demandons-nous une interdiction ?

Premièrement, les systèmes de reconnaissance faciale comportent souvent un aspect discriminatoire, car il a été démontré qu'ils reconnaissent moins bien les personnes racisées ou les femmes, entre autres. Cela se traduit par un nombre plus élevé de faux positifs parmi ces groupes, ce qui peut avoir des conséquences importantes dans le cadre de l'application de la loi, par exemple. Ceci s'explique par le fait que les données avec lesquelles les systèmes ont été entraînés ne sont pas représentatives ou contiennent de manière disproportionnée des données de personnes blanches et d'hommes.

En même temps, une amélioration de la précision au niveau technologique n'élimine pas ce problème. **Deuxièmement, l'utilisation de systèmes de reconnaissance biométrique pour identifier les personnes dans les lieux publics peut permettre une surveillance biométrique de masse qui entre en conflit avec des droits fondamentaux tels que la vie privée, les libertés d'expression et de réunion.** Il s'agit d'empêcher cette surveillance biométrique de masse qui menace nos droits fondamentaux et sape les principes démocratiques fondamentaux.

La présence de cette technologie dans l'espace public crée déjà les conditions nécessaires à la mise en place d'une surveillance biométrique de masse. Les individus ne peuvent pas savoir dans quelles situations, dans quelle mesure et par quels acteurs une reconnaissance biométrique est effectuée, si bien que les effets dissuasifs mentionnés sur les droits fondamentaux se manifestent également lorsque des personnes ne sont pas détectées et identifiées par le système dans une situation donnée. En d'autres termes, même si un système existant n'était effectivement employé pour identifier des personnes que dans des conditions très limitées, la possibilité que cela se produise à tout moment à l'insu des personnes concernées (et même ultérieurement dans certaines circonstances) signifie que la population doit s'attendre à tout moment à être identifiée dans l'espace public. Cela peut conditionner leur comportement, c'est-à-dire que les personnes adapteraient en conséquence leurs actions et leurs mouvements dans l'espace public. Pour cette raison, la création de cette possibilité aurait déjà un potentiel considérable d'entraver gravement l'exercice de droits fondamentaux tels que les libertés de réunion et d'expression.

L'utilisation de ces technologies dans l'espace public ne peut donc pas se faire de manière conforme aux droits fondamentaux, mais est intrinsèquement incompatible avec les droits humains garantis au niveau national et international. Les libertés qui sont menacées par la surveillance biométrique de masse sont indispensables à la participation à la vie publique et au débat public dans une société organisée de manière démocratique. La surveillance biométrique de masse ne constitue donc pas seulement une atteinte aux droits fondamentaux des personnes surveillées, mais porte également atteinte à la sphère publique démocratique dans son ensemble. Les restrictions des droits fondamentaux qu'impliqueraient les systèmes de reconnaissance biométrique dans l'espace public **ne sont donc pas proportionnées.**

stop-reconnaissancefaciale.ch

Une alliance de :
AlgorithmWatch Suisse
Amnesty International Suisse
Société Numérique Suisse



STOP RECONNAISSANCE FACIALE

Demandes

Nous demandons l'interdiction de l'utilisation de systèmes de reconnaissance biométrique dans les espaces accessibles au public en Suisse. Une telle utilisation peut permettre une surveillance biométrique de masse injustifiée, arbitraire ou délibérément discriminatoire et qui n'est pas compatible avec nos droits fondamentaux.

- Cette revendication couvre l'utilisation **par tout type d'acteur** dans les espaces accessibles au public, c'est-à-dire aussi bien les autorités publiques que les acteurs privés.
- Cette demande concerne aussi bien l'utilisation de systèmes de reconnaissance **en temps réel** que **l'utilisation ultérieure** de systèmes de reconnaissance biométrique sur des photos ou des vidéos.
- La demande d'interdiction porte en particulier sur **les systèmes de reconnaissance à distance**, car ils permettent de surveiller des personnes à leur insu et ont donc des effets dissuasifs continus, indépendamment du fait qu'une surveillance soit réellement effectuée ou non. L'interdiction doit également s'appliquer à d'autres systèmes de reconnaissance biométrique si leur utilisation dans l'espace public est susceptible d'entraîner une surveillance de masse.
- Cette revendication concerne **l'espace public**, c'est-à-dire l'espace accessible aux individus sans restrictions. En plus des rues, des trottoirs et des places publiques, cela comprend aussi les parcs, les transports publics - dont les gares et les arrêts - les écoles, les universités, les installations sportives et de loisirs, les stades, les bibliothèques publiques ou les centres commerciaux. Cette liste est bien entendu non exhaustive.

Cette interdiction doit être ancrée juridiquement sur l'ensemble du territoire et garantie politiquement par les autorités.

- Ces deux processus doivent être accompagnés **d'un débat public ouvert**, participatif et fondé sur des faits, dans lequel nous pouvons, en tant que société, discuter de ces lignes rouges dans l'utilisation des systèmes de reconnaissance biométrique et légitimer démocratiquement ces limitations.

A cette fin, nous invitons les communes à ...

- ... interdire l'utilisation de systèmes de reconnaissance biométrique dans les espaces accessibles au public et d'en **interdire légalement l'utilisation par leurs autorités administratives communales**.
- ... prendre la **décision politique** de veiller à ce que les systèmes de reconnaissance biométrique ne soient pas utilisés dans les lieux publics sur le territoire de leur commune. Même s'il n'existe pas de compétence législative communale suffisante pour édicter une interdiction juridique complète (puisque, par exemple, une utilisation par la police se baserait sur la loi cantonale sur la police), une telle décision politique enverrait un signal important.



STOP RECONNAISSANCE FACIALE

Nous demandons aux **cantons** de ...

- ... veiller à ce que **les systèmes de reconnaissance biométrique ne soient pas utilisés dans les espaces accessibles au public.**
- ... s'abstenir de créer des bases légales permettant l'utilisation de systèmes de reconnaissance biométrique.

Au niveau **fédéral**, nous demandons ...

- ... au **corps législatif** d'obtenir une interdiction explicite de l'utilisation de systèmes de reconnaissance biométrique dans les lieux accessibles au public.
- ... à **l'exécutif et l'administration** de s'engager en faveur d'une telle interdiction également au sein des organes et dans les discussions internationales pertinentes.

Arguments de fond

Pourquoi les bases légales actuelles ne sont-elles pas suffisantes ?

La situation juridique initiale exposée ci-dessus montre qu'à l'heure actuelle, l'utilisation de systèmes de reconnaissance biométrique dans l'espace public **n'est en principe pas autorisée en Suisse.** Pour les raisons suivantes, cette réglementation en matière de protection des données **s'avère toutefois insuffisante :**

Elle laisse ouvertes les deux possibilités suivantes ...

(1) ... **les systèmes doivent être utilisés à l'avenir sur la base d'une législation appropriée.**

Le droit de la protection des données pose des exigences particulières à l'utilisation des technologies de reconnaissance biométriques, mais ne les interdit pas par principe ; il fait dépendre leur utilisation de l'existence d'une base légale suffisante. En raison de leur contradiction inhérente avec les libertés garanties par les droits fondamentaux et de l'impossibilité de garantir leur utilisation conforme aux droits fondamentaux, il est indiqué de les interdire formellement dans les espaces accessibles au public.

(2) ... **les systèmes sont malgré tout utilisés de facto, bien que les bases légales n'existent pas ou ne soient pas suffisantes (ce qui, selon l'estimation de plusieurs expert·e·x·s, se produit déjà aujourd'hui).** Afin d'assurer la clarté juridique et d'empêcher de manière fiable cette utilisation dans l'espace public, utilisation qui peut entraîner une surveillance de masse, une interdiction explicite est donc recommandée. Le corps législatif est tenu de préciser avec clarté que l'utilisation de systèmes de reconnaissance biométriques dans l'espace public ne peut pas se faire légalement.

Il est également important de mentionner ici que lors de la première utilisation de nouvelles technologies, la conformité à la protection des données et le principe de finalité sont souvent respectés



STOP RECONNAISSANCE FACIALE

dans un premier temps. Toutefois, une fois que le dispositif technologique - **les systèmes de reconnaissance biométrique dans les lieux publics - est en place, il y a souvent un risque de «mission creep»**. Cela signifie qu'au fil du temps et au fur et à mesure que la technologie se développe, elle est utilisée à d'autres fins et pour répondre à d'autres besoins. Comme cela ne nécessite qu'une adaptation de la base juridique existante (et non la création d'une nouvelle base juridique), le principe initial de finalité est contourné. Dans ce contexte, nous nous engageons à ce qu'aucune base légale ne soit créée pour permettre l'utilisation de systèmes d'identification biométriques.

Les nouvelles technologies peuvent souvent être testées dans le cadre **d'essais pilotes**, ce qui est temporairement autorisé en l'absence de base juridique appropriée. **Après une introduction dans le cadre d'un projet pilote, franchir le pas vers l'ancrage définitif est plus simple**. Ce passage à l'étape suivante est moins perceptible et moins discuté par le public. Les risques liés à l'utilisation de systèmes de reconnaissance biométrique sont trop importants pour que l'on puisse accepter le danger d'une telle introduction dissimulée.

Les risques vont au-delà des aspects liés à la protection des données. La surveillance biométrique de masse menace également la vie privée en tant que telle ainsi que les libertés d'expression et de réunion. Une autorité de protection des données est compétente pour donner des directives à ce sujet, mais non pour effectuer une analyse d'impact générale concernant les conséquences sur les droits fondamentaux, la démocratie et le bien commun. Ces risques ne peuvent pas être convenablement couverts par une analyse de la protection des données.

Pourquoi la reconnaissance biométrique ne pourrait-elle pas être utilisée de manière ciblée à des fins de poursuites judiciaires ?

Le besoin de sécurité, en soi légitime, ne doit pas conduire à une érosion des droits fondamentaux. L'action de l'État est limitée par les droits fondamentaux pour de bonnes raisons, y compris dans le domaine de la poursuite pénale et de la protection de la sécurité publique. Les délits doivent pouvoir être poursuivis par la police et la justice et la sécurité publique doit être préservée - mais cela ne peut se faire qu'au moyen de mesures appropriées et proportionnées. L'État dispose aujourd'hui déjà de moyens importants à cet effet. Pour rappel, une restriction des droits fondamentaux ne peut être justifiée à cette fin que si elle repose sur une base légale, qu'elle est effectuée dans l'intérêt public, qu'elle est proportionnée et qu'elle ne porte pas atteinte à l'essence des droits fondamentaux (art. 36 Cst.).

Cependant, l'utilisation de la reconnaissance faciale automatique et d'autres systèmes de surveillance biométrique dans l'espace public permet une surveillance biométrique de masse qui, comme nous l'avons expliqué plus haut, va au-delà d'une restriction justifiable et proportionnée des droits fondamentaux. Cela dépasse donc le cadre dans lequel les mesures augmen-



STOP RECONNAISSANCE FACIALE

tent la sécurité sans pour autant mettre en danger notre liberté et restreindre nos droits de manière disproportionnée.

Un autre argument contre l'utilisation de systèmes de reconnaissance biométrique dans le cadre des poursuites pénales est qu'ils ne fonctionnent jamais sans erreur. Par exemple, les systèmes de reconnaissance faciale ont tendance à moins bien reconnaître les visages de femmes et de personnes racisées. Il en résulte que ces personnes sont plus souvent confondues, ce qui donne lieu à des **résultats «faussement positifs»**, où le système signale avoir identifié une personne, mais reconnaît en fait une fausse identité. Pour les personnes ainsi faussement identifiées, cela peut avoir de graves conséquences, allant d'un contrôle injustifié, d'un soupçon erroné, à une arrestation arbitraire.

Pourquoi un moratoire ne suffit-il pas ?

Un moratoire n'est pas suffisant pour écarter le risque d'une surveillance biométrique de masse. D'une part, la reconnaissance faciale automatisée progresse lentement, mais il est peu probable qu'elle soit totalement infaillible. D'autre part, et c'est là un point essentiel, on peut certes s'attendre à une amélioration de la précision et de la fiabilité de la technologie, mais cela ne change rien au fait que même une utilisation totalement exempte d'erreur violerait des droits fondamentaux. Les développements techniques ne feraient que transformer ces systèmes en instruments de surveillance encore plus efficaces. Utilisés dans l'espace public, ils restreignent les droits fondamentaux de manière disproportionnée, même - ou surtout - s'ils fonctionnent de manière plus précise.

Et ailleurs ?

En raison du **développement rapide des systèmes de reconnaissance biométrique dans toute l'Europe**, il faut s'attendre à ce que cette évolution se poursuive également en Suisse à défaut d'interventions législatives et de la société civile.

- Plusieurs **villes dans le monde**, dont San Francisco, Portland, ou Nantes, ont interdit l'utilisation de systèmes de reconnaissance faciale dans l'espace public.
- Depuis février 2021, une coalition d'organisations de la société civile appelle également à une interdiction en Europe sous le nom de «[Reclaim Your Face](#)». Au niveau de l'UE, cette coalition a notamment lancé une initiative citoyenne européenne.
- En juin 2021, une coalition internationale de plus de 200 organisations de la société civile, baptisée «[Ban Biometric Surveillance](#)», s'est prononcée dans une lettre ouverte en faveur d'une telle interdiction.
- Au **niveau de l'UE**, le [règlement général sur la protection des données](#) interdit en principe le traitement des données biométriques qui identifient précisément une personne, tout en prévoyant un certain nombre d'exceptions (article 9). La [directive sur la protection des données dans le secteur de la police et de la justice pénale](#) les autorise, sous certaines conditions, à des fins de poursuite pénale (article 10). En avril 2021, la Commission européenne a présenté son projet de [règle-](#)



STOP RECONNAISSANCE FACIALE

ment sur l'intelligence artificielle (AI Act). Il propose d'interdire l'utilisation de systèmes biométriques de reconnaissance à distance en temps réel dans l'espace public par les forces de l'ordre, tout en prévoyant un certain nombre d'exceptions. Le règlement sur l'IA est actuellement en cours de négociation au Parlement européen et au Conseil de l'UE. En octobre 2021, **le Parlement européen s'est prononcé, dans un rapport non contraignant**, en faveur de l'interdiction de l'utilisation de systèmes de reconnaissance biométrique par les forces policières dans l'espace public.

- En septembre 2021, le **Haut Commissariat aux droits humains de l'ONU** s'est également prononcé dans un **rapport** en faveur d'une limitation substantielle ou d'une interdiction de l'utilisation de systèmes de reconnaissance biométrique dans les lieux publics.
- En décembre 2021, la nouvelle coalition gouvernementale en Allemagne s'est prononcée dans son **accord de coalition** pour "exclure la reconnaissance biométrique dans l'espace public (...) en vertu du droit européen".

Campagne stop-reconnaissancefaciale.ch

Il est essentiel que les garde-fous et les lignes rouges de l'utilisation des systèmes de reconnaissance biométrique soient définis dans le cadre d'un débat sociopolitique et que des règles claires soient établies avant que ces systèmes ne soient utilisés à grande échelle.

C'est dans ce contexte que les trois organisations de la société civile **AlgorithmWatch Suisse**, **Amnesty International Suisse** et **Société Numérique Suisse** ont lancé la campagne **stop-reconnaissancefaciale.ch**. Dans un premier temps, la coalition récolte des signatures dans une pétition en ligne pour interdire la reconnaissance faciale automatisée dans les espaces publics des villes suisses.

La campagne est soutenue par des **personnes issues du monde politique, de la société civile et du monde scientifique**.

Plus d'informations :

www.stop-reconnaissancefaciale.ch | office@stop-reconnaissancefaciale.ch



ALGORITHM
WATCH / CH

AMNESTY
INTERNATIONAL



SOCIÉTÉ
NUMÉRIQUE

stop-reconnaissancefaciale.ch

Une alliance de :

AlgorithmWatch Suisse
Amnesty International Suisse
Société Numérique Suisse