



Date de dépôt : 15 mai 2023

Rapport

de la commission judiciaire et de la police chargée d'étudier la proposition de motion de Bertrand Buchs, Jacques Blondin, Claude Bocquet, Patricia Bidaux, Jean-Charles Lathion, Guy Mettan, Sébastien Desfayes, Salika Wenger, Boris Calame, Glenna Baillon-Lopez, Charles Selleger, François Lefort, Didier Bonny, Marta Julia Macchiavelli, Philippe de Rougemont, Anne Bonvin Bonfanti, Marjorie de Chastonay, Katia Leonelli, Pierre Eckert, Philippe Poget, Yves de Matteis pour l'interdiction de la technologie de reconnaissance faciale dans l'espace public genevois et à l'intérieur des bâtiments de l'administration cantonale

Rapport de Alberto Velasco (page 3)

Proposition de motion (2891-A)

pour l'interdiction de la technologie de reconnaissance faciale dans l'espace public genevois et à l'intérieur des bâtiments de l'administration cantonale

Le GRAND CONSEIL de la République et canton de Genève
considérant :

- les articles 13 et 36 de la Constitution suisse ;
- les articles 18 et 21 de la constitution de la République et canton de Genève ;
- l'absence de bases légales concernant l'utilisation de la reconnaissance faciale ;
- l'absence de débat public concernant l'utilisation de la reconnaissance faciale ;

vu :

- l'interdiction de la reconnaissance faciale sur le territoire public décidée par les villes de San Francisco et Oakland ;
- les propositions de la Commission européenne du 21 avril 2021 ;
- la réponse du Conseil fédéral à l'interpellation de M. Balthasar Glättli (parti écologiste suisse) du 5 mai 2021,

invite le Conseil d'Etat

à interdire la technologie de reconnaissance faciale sur le domaine public genevois, à l'intérieur des bâtiments de l'administration cantonale et dans les gares.

Rapport de Alberto Velasco

La commission judiciaire et de la police a traité cet objet lors de sa séance du 27 avril 2023, sous la présidence de M. Sébastien Desfayes.

Le procès-verbal a été rédigé par M. Clément Magnenat.

La commission a été assistée dans ses travaux par son secrétaire scientifique, M. Jean-Luc Constant (SGGC).

Introduction

L'auteur de cette motion indique dans son exposé des motifs les éléments suivants :

En 2019, les villes de San Francisco et Oakland ont interdit l'utilisation de la reconnaissance faciale dans leur espace public. Elles ont argumenté sur le fait que *« la propension de la technologie de reconnaissance faciale à mettre en danger les libertés civiles surpasse substantiellement ses bénéfices supposés, la technologie va exacerber les injustices raciales et menacer notre capacité à vivre libres de la surveillance permanente du gouvernement »*.

Les études ont clairement démontré que cette technologie entraînait de multiples erreurs au sein d'une population noire ou asiatique.

La Commission européenne a présenté le 21 avril 2021 ses propositions pour réglementer l'intelligence artificielle. Il est ainsi prévu d'interdire l'identification biométrique à distance en temps réel dans l'espace public, y compris pour les forces de l'ordre, mais l'utilisation de la reconnaissance faciale restera autorisée dans certaines circonstances.

Il faut signaler qu'Interpol utilise cette technique avec la collaboration de la majorité des pays du monde.

Pour ce qui est de la Suisse, la loi révisée sur la protection des données (révLPD), qui est entrée en vigueur le 1^{er} janvier 2022, qualifie de données sensibles les données biométriques identifiant un physique de manière univoque.

Le conseiller national Balthasar Glättli (parti écologiste suisse) a déposé le 5 mai 2021 une interpellation au Conseil fédéral demandant sa position concernant cette nouvelle technologie au regard de la révision de la LPD.

Dans sa réponse du 11 août 2021, le Conseil fédéral rappelle que la nouvelle LPD range les données biométriques dans les données sensibles. Ce faisant, elle met en œuvre le Protocole d'amendement (STCE n° 223) à la Convention pour la protection des personnes à l'égard du traitement automatisé

des données personnelles (Convention 108+) qui n'autorise le traitement de telles données que moyennant des garanties appropriées. Il définit les données biométriques comme des technologies traitant les empreintes digitales, les images faciales, les images de l'iris ou encore la reconnaissance de la voix. Il considère que la nouvelle LPD garantit une protection suffisante pour le traitement des données ayant recours à la reconnaissance faciale qui pourrait être effectuée par les autorités fédérales et les particuliers.

Cette LPD ne s'applique en revanche pas aux traitements de données par les organes cantonaux. Ces autorités disposent d'une marge de manœuvre pour recourir à la reconnaissance faciale, mais doivent respecter les articles 13 et 36 de la Constitution suisse et les exigences de la Convention 108+ que la Suisse s'apprête à ratifier.

Dans un arrêt (146 | 11), le Tribunal fédéral a considéré que l'enregistrement de données d'identification par les autorités cantonales à partir des plaques d'immatriculation dans le cadre d'un système de surveillance du trafic, et le fait de les combiner en l'espace de quelques secondes avec d'autres banques de données, constituait une atteinte à l'article 13, alinéa 2 de la Constitution suisse.

Le Tribunal fédéral a estimé que, dans le cas d'espèce, la base légale n'était pas suffisante. Pour le Conseil fédéral, les exigences posées par le Tribunal fédéral s'appliqueraient a fortiori si les autorités cantonales avaient recours à un système de surveillance et d'identification par reconnaissance faciale.

Pour le Conseil fédéral, une interdiction absolue ou un moratoire ne sont pas à l'ordre du jour, mais il admet qu'un canton pourrait légiférer sur cette question.

Pour les raisons qui ont été expliquées et étant donné la liberté laissée aux cantons de légiférer, les motionnaires demandent à ce que le Conseil d'Etat interdise la reconnaissance faciale dans l'espace public et à l'intérieur des bâtiments de l'administration cantonale.

Travaux de la commission

Auditions

Audition de M. Bertrand Buchs, premier signataire

M. Buchs commence par indiquer que cette proposition de motion est très simple et qu'elle ne contient qu'une seule invite, dont il fait la lecture : « *interdire la technologie de reconnaissance faciale sur le domaine public genevois et à l'intérieur des bâtiments de l'administration cantonale* ». Cette motion a été déposée, car les députés se sont rendu compte qu'il manquait des

bases légales sur les questions de la reconnaissance faciale. Certaines villes aux Etats-Unis l'ont déjà interdite. Cette thématique a fait l'objet de discussions au niveau fédéral. En effet, une interpellation a été déposée par un conseiller national du parti des Verts. Le Conseil fédéral a répondu à cette interpellation en indiquant que tout dans ce domaine était en chantier. Or, la plupart des caméras de vidéosurveillance qui sont vendues actuellement contiennent d'ores et déjà un logiciel capable de faire de la reconnaissance faciale. Par ailleurs, dans un article du 14 avril 2023 du journal *Le Temps*, l'essor fulgurant de la vidéosurveillance est mis en avant. En théorie, toutes les caméras de surveillance doivent être répertoriées, mais la plupart ne le sont pas, comme le démontre cet article de presse. La réponse du Conseil fédéral est très claire : il indique que tout système doit respecter les articles 13 et 36 de la Constitution fédérale. Il faut donc faire attention à ces deux bases légales. De plus, un accord international s'applique en la matière. Il s'agit de la Convention 108 + (Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel). Cette convention prévoit que les données biométriques doivent être régies par des lois très claires. La Suisse a signé cette convention. La Suisse doit également respecter la révision de la loi sur les données qui prévoit que les données sensibles doivent être surveillées et protégées. Le cadre légal ne va pas plus loin au niveau fédéral, mais les cantons disposent d'une marge de manœuvre. Face à la réponse du Conseil fédéral à l'interpellation de 2011, Genève dispose de la marge nécessaire en tant que canton pour légiférer sur cette question.

M. Buchs estime qu'il est urgent de légiférer sur cette nouvelle pratique, notamment parce que ces logiciels commettent des erreurs au niveau de la reconnaissance faciale. Ces erreurs concernent surtout les personnes noires et les personnes asiatiques. Il mentionne également la polémique concernant les CFF, qui ont exprimé le souhait d'introduire la reconnaissance faciale dans les gares uniquement pour booster les marchés. Si une régie fédérale commence à utiliser ces données pour des raisons économiques sans demander l'autorisation des personnes concernées, cela représente un danger qu'il convient d'appréhender sur le plan législatif. Il souhaite donc que le Grand Conseil se saisisse de ce sujet pour adopter des cautèles.

Questions des commissaires

Pour que la reconnaissance faciale soit possible, il faut disposer d'une base de données qui contienne l'ensemble des visages de la population. Si seul l'Etat dispose de cette base de données, la question d'un commissaire est la suivante : qui d'autre serait en mesure de l'utiliser ?

M. Buchs indique que ces bases de données s'auto-entretiennent grâce à l'intelligence artificielle. Par conséquent, les grandes entreprises ont également accès à ces bases de données. Les Israéliens et les Chinois sont à la pointe sur ce genre de systèmes. Or, ces logiciels de reconnaissance faciale ne sont pas optimaux pour certaines ethnies. Il est en effet arrivé aux Etats-Unis que la reconnaissance faciale reconnaisse une personne noire, alors que cette dernière n'avait rien à voir avec le cas en question.

Le même commissaire indique que la Chine dispose des photos de l'ensemble de ses ressortissants et il demande s'il est possible, en Suisse, en systématisant les photos qui se trouvent sur le net, de créer une base de données similaire dans laquelle l'ensemble des visages seraient répertoriés.

M. Buchs répond par l'affirmative et donne l'exemple de l'utilisation de la reconnaissance faciale pour débloquer les téléphones portables : certains téléphones peuvent s'ouvrir via la reconnaissance faciale. En tant que consommateur, lorsqu'on clique pour indiquer que l'on est d'accord avec les conditions d'utilisation sans les lire, on ne sait pas où finissent nos données personnelles.

Un commissaire se demande, s'agissant de l'usage de ces nouvelles technologies, s'il faut les interdire ou s'il ne faudrait pas plutôt tenter de maîtriser le phénomène. Plutôt que d'interdire, il demande s'il ne faudrait pas plutôt adopter une voie qui permettrait de s'assurer que l'on dispose des bases légales nécessaires pour contrôler l'utilisation de ces logiciels. Il estime que l'on ne pourra de toute façon pas colmater toutes les brèches.

M. Buchs partage totalement cet avis. La reconnaissance faciale est utilisée dans certaines situations par l'Etat, notamment face aux risques de terrorisme. Selon lui, il est tout à fait justifié de pouvoir utiliser ces logiciels lorsqu'on doit arrêter quelqu'un de manière très urgente. Mais cette motion a pour but de faire réagir le politique sur cette thématique. Sur la solution à suivre et sur la législation à adopter, la motion reste très souple. Selon lui, il est très préoccupant que les CFF veuillent utiliser la reconnaissance faciale à des fins commerciales. Le législateur est très en retard sur ces questions. Ces domaines avancent très vite et l'utilisation qui est faite de la reconnaissance faciale dans le privé est de plus en plus importante. Or, l'Etat n'a aucun contrôle sur ce que font les privés dans ce domaine.

Quant à savoir s'il n'est pas trop tard pour légiférer en ce sens sur ces avancées technologiques, M. Buchs considère qu'en politique, il n'est jamais trop tard et que, si l'on ne se saisit pas de ces questions, alors ce sera vraiment trop tard.

Considérant que l'intelligence artificielle augmente largement le danger, un commissaire demande à M. Buchs s'il a connaissance d'exemples de dangers en lien avec l'utilisation de tels logiciels.

M. Buchs explique que les tests qui ont été effectués en 2019 et 2020 ont démontré que les logiciels reconnaissaient beaucoup mieux les visages des personnes à peau blanche. Cela s'explique peut-être par un biais des données à disposition pour conduire lesdits tests. Ce qui est sûr, c'est que les systèmes qui s'autogénèrent se trompent nécessairement à un moment donné. Il se demande si, à l'avenir, l'on aura encore le droit de critiquer les résultats qui proviennent de la reconnaissance faciale ou si l'on fera une confiance aveugle à ce type de logiciels.

Le même commissaire donne l'exemple du gouvernement italien qui a demandé l'extradition de France d'un pizzaiolo identifié grâce à la reconnaissance faciale comme étant un criminel calabrais recherché depuis 10 ans. Cela démontre la puissance de la reconnaissance faciale, mais également ses dangers. Il demande à M. Buchs s'il dispose de données sur les risques de piratage que représentent ces systèmes.

M. Buchs n'a pas d'exemple précis à donner. L'on sait que beaucoup de données sont présentes sur le darknet. Il n'a pas de chiffres précis à présenter à la commission, mais il estime que les cas de piratages de ces logiciels sont extrêmement probables. Il cite l'exemple des données médicales : il arrive que ces dernières soient vendues, car elles intéressent beaucoup de monde. Il revient ensuite sur l'utilisation de la reconnaissance faciale pour débloquent les téléphones portables et invite les commissaires à ne pas le faire, expliquant que cela participe à l'alimentation des bases de données qui sont utilisées dans le cadre de la reconnaissance faciale.

Le président estime qu'un progrès doit encore être réalisé pour ces logiciels, tout en constatant que l'intelligence artificielle offre des résultats fascinants. Il revient sur les exemples d'erreurs qui ont été commises aux Etats-Unis, mentionnés par M. Buchs, et il lui demande si ces exemples ne posent pas la question du développement d'une société totalitaire.

M. Buchs répond par l'affirmative et indique que c'est précisément cela qui l'inquiète le plus. Selon lui, l'on est en train d'assister à un changement de paradigme qui a pour conséquence que la société n'a plus de pouvoir sur ces données. Si l'Etat n'a rien à dire là-dessus, alors la politique se doit de reprendre le dessus pour stopper le développement de ces pratiques. L'Europe a décidé de prendre des décisions en ce sens, mais les processus sont très longs. Selon lui, un texte devrait être voté sur l'usage qui est fait de la reconnaissance

faciale. C'est un sujet qui doit en urgence être pris en charge par les cantons, ainsi que par la Confédération.

Ensuite, le président revient sur l'invite de la motion qui vise à interdire la technologie de la reconnaissance faciale sur le domaine public et il demande à M. Buchs de confirmer qu'à l'heure actuelle, cette technologie n'est pas utilisée par les autorités du canton.

M. Buchs le confirme et il ajoute par ailleurs qu'une étude menée dans le quartier des Pâquis avait démontré que la présence de caméras de vidéosurveillance ne servait pas à grand-chose pour les autorités.

Quant au fait de faire une distinction entre la reconnaissance faciale et les caméras de vidéosurveillance, M. Buchs est d'accord qu'il s'agit de deux technologies différentes, mais il rappelle que les caméras de vidéosurveillance qui sont vendues actuellement contiennent déjà le logiciel permettant d'utiliser la reconnaissance faciale. Si l'on dispose de l'outil, alors pourquoi ne pas l'utiliser ? A la suite de quoi, le président en déduit qu'il suffirait à l'Etat de prendre les images issues de la vidéosurveillance et de les soumettre aux logiciels qui font de la reconnaissance faciale pour recevoir des indications sur les déplacements des personnes en question, et M. Buchs note que cette pratique est celle utilisée par les Chinois. En Chine, si l'on traverse au rouge, on perd des points. Cette opération se fait en temps réel. Ces logiciels fonctionnent déjà et fonctionneront de mieux en mieux. Selon lui, le système est d'ores et déjà incontrôlable. Il recommande aux membres de la commission de lire l'article du Temps qu'il a mentionné précédemment. Il propose également à la commission d'entendre l'association qui a conduit l'étude sur les caméras de vidéosurveillance non répertoriées à Genève. Selon lui, si l'Etat ne réagit pas maintenant, alors il sera trop tard.

Au sujet, de l'atteinte grave à la protection de la sphère privée qui est au centre de cette thématique, M. Buchs indique que la loi sur les données est très stricte et que des cauteles existent, mais les Etats sont complètement dépassés par cette problématique.

Sur le fait que l'invite témoigne d'une sorte d'impuissance politique, car actuellement l'exploitation commerciale de ces outils par les sociétés multinationales du numérique à Genève est totalement incontrôlable, M. Buchs constate que le politique est naïf sur ces questions, car en vérité on ne sait pas ce qui se passe dans le privé. L'on a toutes et tous donné à des entreprises privées nos données ; or, on ne sait pas ce que font de nos données ces entreprises qui fonctionnent en dehors de l'Etat.

Au sujet des perspectives extraordinaires qui sont ouvertes grâce à ces progrès, M. Buchs estime quant à lui que le seul aspect positif que représente

la reconnaissance faciale concerne la recherche de grands criminels, notamment de terroristes. Il reconnaît que cela peut être un côté positif pour la sécurité de l'Etat. A la suite de quoi, le président note que parmi les côtés positifs, il y a aussi les perspectives qu'offre le développement de l'intelligence artificielle.

Un commissaire fait une réflexion générale sur la gravité de ces évolutions technologiques qui échappent. Aujourd'hui, la société est scannée en permanence. Ce qui était de la science-fiction il y a quelques années encore est devenu notre réalité. Il se demande s'il ne serait pas possible d'interdire l'utilisation de la reconnaissance faciale à des fins commerciales. Tous les systèmes commerciaux font signer des accords sur la base de l'acceptation des conditions générales. Personne ne lit jamais le descriptif de ces conditions, car, en tant que consommateur, l'on a envie de pouvoir utiliser l'outil tout de suite. Etant donné qu'on ne peut pas consentir à quelque chose qui est contraire à la loi, il se demande si l'on ne devrait pas aller plus loin et considérer que la reconnaissance faciale à des fins commerciales est interdite. Cela voudrait dire que la reconnaissance faciale reste possible pour les questions sécuritaires, mais pas à des fins commerciales. La reconnaissance faciale peut avoir des vertus et des utilités, mais elle devrait être cantonnée à une utilisation de sécurité publique.

M. Buchs indique qu'il est entièrement d'accord avec cette approche. Toutes les nouvelles technologies doivent être utilisées à bon escient et de manière cadrée. Le temps législatif ne permet pas d'être pro-actif, car pour ce qui est des nouvelles technologies, la politique réagit avec des années de retard. Il ne sait pas s'il est possible au niveau juridique d'agir sur le domaine privé. Il se demande s'il est par exemple possible de légiférer pour empêcher quelqu'un de placer une caméra de vidéosurveillance sur sa propriété.

Un autre commissaire retient des propos de M. Buchs principalement les risques d'erreur évoqués dans le cadre de l'utilisation de la reconnaissance faciale aux Etats-Unis. Il souligne qu'indépendamment des perfectionnements de ces technologies, l'erreur reste possible. Or, plus on est certain que le logiciel est infailible, plus l'erreur coûte cher à la personne qui est victime, car on remettra de moins en moins en cause la fiabilité du logiciel en question. Il donne l'exemple d'un épicier allemand qui avait été enlevé par les services secrets américains. Ces derniers s'étaient ensuite rendu compte qu'il s'agissait d'une erreur. Le danger de ces technologies réside aussi dans la confiance qu'on aura dans ces logiciels. Le même constat a été fait pour le bornage des téléphones : étant donné que la police utilise systématiquement cette information, les malfrats remettent désormais leurs téléphones à d'autres personnes avant de se rendre sur le lieu de l'infraction afin de pouvoir avoir un

alibi factice à présenter à la police en cas d'arrestation. Il mentionne également les masques qui sont devenus plus habituels depuis la crise du covid et qui permettent de dissimuler le visage. Si l'on utilise la reconnaissance faciale de manière plus fréquente, alors l'on pourrait être soupçonné de vouloir commettre un acte illégal juste parce qu'on se dissimule le visage en portant un masque.

M. Buchs ajoute que le grand risque est qu'on nous vole notre identité. Il est arrivé que des gens se retrouvent à devoir prouver qui ils étaient sans y parvenir. Ces situations peuvent être extrêmement angoissantes, car l'on n'a plus le pouvoir sur la technologie qui est utilisée. Si l'on ne réagit pas maintenant, l'on se retrouvera dans un système où il ne nous sera plus possible de réagir.

On fait remarquer à M. Buchs que la Commission européenne a examiné un texte qui vise à interdire l'usage de la reconnaissance faciale par les forces de l'ordre. A l'heure actuelle, les forces de l'ordre utilisent cette technologie, mais cela sera interdit par ce nouveau texte européen. Ce qu'il confirme en indiquant que cette réflexion est en cours, mais il souligne que cela se passe au niveau européen et que le texte en question n'a pas encore été voté.

Quant au fait que le texte européen prévoit que l'utilisation de la reconnaissance faciale restera possible dans certaines circonstances, M. Buchs indique qu'il s'agit des situations en lien avec des actes de terrorisme.

Un des commissaires relève que les villes de Saint-Gall, de Zurich et de Lausanne ont pris des mesures pour interdire la reconnaissance faciale.

A la suite de cette audition, la commission délibère en statuant sur la nécessité de procéder à certaines auditions.

Trois groupes, Verts, S, et PL, proposent de renvoyer directement cette motion au Conseil d'Etat.

A la suite de quoi, le représentant du département estime qu'il serait intéressant pour la commission d'entendre le préposé cantonal à la protection des données, qui pourra présenter les principes qui encadrent cette pratique. Le profilage facial n'est actuellement pas autorisé. Dès lors, il convient de se demander s'il est important d'interdire quelque chose qui n'est pas autorisé, étant donné que, dans le système actuel, une autorisation est nécessaire pour pouvoir avoir recours à la reconnaissance faciale. Selon lui, il serait bien d'entendre le spécialiste.

Le groupe S relève que la motion ne fait qu'inviter le Conseil d'Etat à se pencher sur une loi en la matière. Selon lui, la commission peut décider d'auditionner à ce stade, mais elle peut également directement renvoyer cette motion au Conseil d'Etat pour voir s'il souhaite légiférer ou pas. Il considère

que la présentation de M. Buchs est suffisamment éclairante à ce stade. Si la commission décide de renvoyer directement au Conseil d'Etat, alors il y aura une loi si le Conseil d'Etat décide d'en faire une. S'il n'y a pas de loi, alors tout sera permis. Or, les dangers présentés par M. Buchs sont à prendre en considération aussi vite que possible et de ce fait cette motion mérite d'être votée.

Pour le groupe des Verts, il est fort possible que l'outil proposé participe à la rédaction de la loi proposée par le Conseil d'Etat.

Le groupe EAG revient sur les propos du département selon lesquels « ce qui n'est pas autorisé n'est pas nécessairement interdit ». Si l'on prend une photo d'un ami dans la rue et que des gens se trouvent derrière cet ami, si l'ordinateur sur lequel je poste cette photo reconnaît ces personnes, alors je fais de la reconnaissance faciale. La question se pose donc de savoir si cela constitue ou non un délit. Selon lui, il faut adopter une disposition légale pour interdire l'utilisation de la reconnaissance faciale pour les personnes qui se promènent simplement dans la rue. Dès lors que le texte en question est une motion, il propose de l'envoyer au Conseil d'Etat. Selon lui, il est important de prévoir des dispositions pour cadrer ce type de risques.

Le groupe MCG indique qu'il est embêté par cette motion qui vise, in fine, à interdire la reconnaissance faciale. Genève a beaucoup de lois qui ne sont pas appliquées ou peu appliquées. Il craint que ce texte ne consiste qu'à se faire plaisir en lançant un grand principe qui n'est en réalité pas applicable, ce qui n'est jamais une bonne chose pour le pouvoir législatif. La vidéosurveillance est très cadrée à Genève, mais il est vrai que les smartphones rendent très accessibles les atteintes à la sphère privée. Pour le MCG, cette interdiction risque plus de poser des problèmes que d'apporter des solutions. C'est une loi qui fera plaisir à ceux qui la voteront, mais qui n'aura que peu d'efficacité. Il trouve utile d'entendre le préposé à la protection des données et à la transparence afin d'essayer de proposer quelque chose de plus fin. Une autre possibilité serait de proposer de modifier la législation actuelle et ainsi d'agir non pas par un texte déclaratif, mais par quelque chose d'effectif. Il souligne que la Confédération continue à se placer en dehors des lois, car les CFF proposent une utilisation de la reconnaissance faciale qui est hors du droit. En l'état, il estime qu'il est prématuré de voter cette motion et qu'il convient, au minimum, d'auditionner le préposé à la protection des données.

Un commissaire du groupe S revient sur l'exemple donné par le groupe EAG et sur la distinction entre ce qui n'est pas autorisé et ce qui est interdit : si l'on prend une photo de quelqu'un dans la rue avec son téléphone, si une loi interdit cette pratique, alors cet acte est hors la loi. A l'inverse, s'il n'y a pas de loi qui l'interdit, alors tout le monde peut le faire. Ce que ce texte veut éviter

c'est qu'on se retrouve avec des caméras qui nous scannent dans la rue et dans les magasins qui récoltent des informations. Le but est donc d'élaborer une loi qui interdise cette pratique. Que cela soit techniquement impossible ou pas est un autre problème. L'idée est simplement d'avoir une loi pour permettre aux personnes de se défendre face à ces techniques. La motion demande simplement au Conseil d'Etat de légiférer.

Le département, à propos de la question de la base légale formelle qui est actuellement demandée pour que le profilage soit autorisé, précise que cette pratique n'est pas autorisée, mais elle n'est pas interdite non plus. Elle est possible uniquement s'il y a une autorisation. Ici, le texte vise surtout à réprimer un comportement. Il s'agit de pénaliser les comportements qu'on ne souhaite pas voir. Il faut se demander si c'est une infraction que d'utiliser ces données. En Suisse, il n'y a pas d'infraction sur l'usurpation d'identité. L'usurpation d'identité est réprimée uniquement dans le cas d'un usage de faux. Si l'on veut interdire un comportement en particulier, alors il s'agit de créer une base légale pénale. C'est ici que se trouve la différence entre « l'interdit » et « le non-autorisé ».

Un commissaire du groupe des Verts entend les oppositions et la résistance exprimée par le représentant du département. Il tient à rappeler que le texte en question n'est pas un projet de loi. Il s'agit d'une motion qui demande au Conseil d'Etat d'analyser les possibilités de créer une base légale. Il entend que le département donne déjà une partie de sa réponse. Il demande que la motion soit votée afin que la réponse du Conseil d'Etat soit formalisée. Il propose donc que la commission vote sur la proposition de voter ce texte dès à présent.

Le commissaire S reconnaît que la reconnaissance faciale est possible sur son téléphone. Mais comme il n'y a aucune loi qui l'interdit, il ne peut rien faire pour se protéger contre l'utilisation qui peut être faite de la reconnaissance faciale. Il souhaite qu'une loi soit adoptée pour que des plaintes soient possibles.

<p>Sans autre commentaire le président met d'abord aux voix l'audition du préposé cantonal à la protection des données, qui est refusée par : 4 oui (1 PDC, 1 UDC, 2 MCG), 7 non (1 EAG, 2 S, 2 Ve, 2 PLR) et 0 abst.</p>
--

A la suite de quoi, le groupe MCG propose d'ajouter « et dans les gares » à la fin de l'invite. Ainsi, le Conseil d'Etat dira si le canton a la compétence ou non de légiférer sur les gares afin de viser également la pratique envisagée par les CFF.

Mis aux voix, l'amendement à l'invite de la motion :

« à interdire la technologie de reconnaissance faciale sur le domaine public genevois, à l'intérieur des bâtiments de l'administration cantonale et dans les gares ».

est accepté par :

7 oui (2 S, 2 PLR, 1 UDC, 2 MCG), 4 non (1 EAG, 2 Ve, 1 PDC) et 0 abst.

A la demande d'un commissaire de savoir si l'invite parle de l'espace public ou du domaine public, le président confirme que l'invite vise le domaine public.

Mise aux voix, la M 2891 ainsi amendée **est acceptée** par :

10 oui (1 EAG, 2 S, 2 Ve, 2 PLR, 1 UDC, 1 MCG, 1 PDC), 0 non et 1 abst. (1 MCG)

Conclusion

Mesdames et Messieurs les députés, eu égard aux éléments qui vous ont été exposés ci-dessus et du vote intervenu, la majorité de la commission judiciaire et de la police vous recommande de lui faire bon accueil.