Observations sur le

Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement à la reconnaissance faciale

publié par les autorités de protection des renseignements personnels au Canada

Présentées par
Céline Castets-Renard

Avec la collaboration de
Pierre-Luc Déziel
Lyse Langlois

OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE

CHAIRE DE RECHERCHE
I.A. RESPONSABLE À L'ÉCHELLE MONDIALE

Ces observations sont présentées par :

- **Céline Castets-Renard**, professeure titulaire à la Faculté de droit civil de l'Université d'Ottawa, titulaire de la chaire de recherche IA responsable à l'échelle mondiale, coresponsables de l'axe Relations internationales, action humanitaire et droits humains de l'OBVIA. ccastets@uottawa.ca.

Avec la collaboration de :

- **Pierre-Luc Déziel**, professeur agrégé à la Faculté de droit de l'Université Laval, coresponsable de l'axe Droit, cyberjustice et cybersécurité de l'OBVIA. pierre-luc.deziel@fd.ulaval.ca ;
- **Lyse Langlois**, Professeure titulaire à la Faculté des sciences sociales de l'Université Laval, directrice générale de l'Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique (OBVIA) et directrice de l'Institut d'éthique appliquée (IDÉA). lyse.langlois@observatoire-ia.ulaval.ca.

.

OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE

CHAIRE DE RECHERCHE I.A. RESPONSABLE À L'ÉCHELLE MONDIALE

Québec

Fonds de recherche – Nature et technologies
Fonds de recherche – Santé
Fonds de recherche – Société et culture

ISBN: 978-2-925138-07-5

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2021.

OBSERVATIONS SUR LA VERSION PRÉLIMINAIRE DU DOCUMENT D'ORIENTATION

1. Le présent document d'orientation aura-t-il l'effet escompté, soit de contribuer à assurer que l'usage que font les services de police de la RF est légal et atténue comme il se doit les risques d'atteinte à la vie privée? Si vous estimez que ce n'est pas le cas, pourquoi?

Le document d'orientation est particulièrement riche et documenté. Il est utile à la compréhension mais on peut identifier plusieurs limites.

Sur la forme, il est sans doute trop long et dense. Il mêle en outre différents genres stylistiques et approches sur le fond du sujet : rappel des législations sur les renseignements personnels et de la jurisprudence sur le fondement de l'article 8 de la Charte canadienne des droits et libertés ; explications théoriques sur les aspects légaux, éthiques et techniques ; réflexions sur des interprétation à retenir pour chercher des solutions légales en *common law* par exemple ; conseils plus concrets et pragmatiques sur le recours à cette technologie et les conditions du choix des prestataires et de leurs services. Le niveau d'explication est très technique, tant au plan du droit que de la technologie, et devrait être simplifié.

L'ensemble de ces explications est donc long, complexe, mais aussi source de confusion pour des services de police qui disposent de peu de temps. On peut fortement douter qu'ils puissent avoir le temps nécessaire pour en prendre correctement connaissance et même le comprendre.

Enfin, certains développements ne sont pas directement utiles à la pratique policière et si la « culture générale » en la matière peut être intéressante, on peut douter de sa pertinence dans un « document d'orientation » qui paraît être parfois un « document d'explication et de réflexion » plutôt qu'un guide opérationnel. Un guide de bonnes pratiques concret et précis serait sans doute plus utile. Il permettrait en outre de rentrer dans plus de détails utiles sur la mise en œuvre portant en particulier sur la documentation technique qui devrait obligatoirement accompagner les systèmes de reconnaissance faciale, qu'ils soient créés en interne ou par des entreprises externes.

En résumé, il serait souhaitable de simplifier, écourter et de ne pas élaborer un document trop général mais plus direct et opérationnel, si on veut espérer pouvoir aider les polices dans leur mission. Il serait également souhaitable d'organiser des formations et accompagnements pour les professionnels afin de développer en particulier une compétence éthique et des bases juridiques.

2. Le présent document d'orientation peut-il être mis en œuvre concrètement?

Voir la réponse ci-dessus. Ce document paraît plus être une explication détaillée des enjeux techniques, éthiques et juridiques, ainsi que des règles légales applicables qu'un outil directement applicable. La liste de recommandations à la fin est toutefois plus claire et concise et tend à prévoir des règles à suivre. Ce document d'orientation devrait surtout

déterminer et présenter un « mode opératoire » dans l'utilisation de la RF conforme au droit et à l'éthique qui serait utile aux services de police plutôt que de présenter une analyse juridique combinant un simple rappel du droit et réflexion plus théorique.

À quelles pratiques et techniques exemplaires les organismes d'application de la loi pourraient-ils avoir recours pour mettre en pratique le présent document d'orientation? Dans les cas où la mise en application pourrait s'avérer difficile, veuillez en expliquer les raisons et fournir des exemples ainsi que des renseignements détaillés dans la mesure du possible.

En l'état, la mise en application du texte parait difficile car il n'est pas assez concret et opérationnel. Nous suggérons de partir des recommandations et d'aider à leur mise en œuvre pratique en les accompagnant des spécifications techniques qui devraient être requises et fournies dans une documentation technique. Par exemple, pourrait être suivie la démarche de la proposition de règlement sur l'IA de la Commission européenne qui pose des règles portant sur le système de gestion des risques (article 9) et sur la gouvernance des données (article 10). Le respect de ces obligations sera contrôlé au travers d'une documentation technique à informer par le fournisseur de systèmes d'IA conformément aux spécifications prévues à l'annexe IV. Ces mesures peuvent être une source d'inspiration sur la méthode à suivre pour encadrer l'usage de la RF par la police mais aussi sur le fond des règles. L'outil d'un « guide de bonnes pratiques » nous semble plus adapté qu'un document d'orientation qui semble poursuivre plusieurs objectifs dont orienter le respect du droit des renseignements personnels.

3. Les recommandations figurant à la section « Exactitude » suffisent-elles pour s'assurer que les services de police s'acquittent de leurs obligations en matière d'exactitude dans les initiatives faisant intervenir la RF? Dans votre réponse, nous vous invitons à formuler des observations sur les pratiques exemplaires permettant de fixer un seuil approprié pour les correspondances de RF et de déterminer les taux d'erreur acceptables, le cas échéant.

Cette partie explicative est intéressante et pédagogique mais ne donne pas de moyens concrets pour décider comment mettre en œuvre ces taux d'exactitude et déterminer ce qui est acceptable ou non. En outre, plutôt que d'imposer ou vouloir poser un « seuil approprié » qui le plus souvent dépend du contexte, il vaudrait mieux mettre en œuvre une procédure ou des moyens de contrôle à la disposition des services de police pour déterminer au cas par cas les conséquences des résultats produits et vérifier si elles sont acceptables ou non, suivant les circonstances. Mieux vaudrait mettre en place des bonnes pratiques et procédures de contrôle (output) pour vérifier l'impact sur les populations avant utilisation et déploiement. Il convient de mettre en œuvre ces mesures dans un « bac à sable » pour expérimenter en amont tout déploiement dans le monde réel.

4. Les recommandations du document d'orientation portant sur la conservation et la destruction des renseignements personnels recueillis et utilisés dans le cadre d'une initiative de RF peuvent-elles être mises en œuvre de manière appropriée dans un contexte d'application de la loi? Si ce n'est pas le cas, pourquoi?

Ces recommandations nous semblent conformes à un contexte d'application de la loi. Elles semblent même davantage s'adresser aux juges et avocats plutôt qu'aux services de police qui risquent d'être dépassés par ces nombreuses et vastes considérations légales (voir ci-dessus).

5. À quelles mesures ou pratiques les services de police peuvent-ils avoir recours pour veiller à ce que toute tierce partie prenant part à une initiative de RF soit légalement autorisée à exercer ses activités? Par tierces parties, on entend, par exemple, des fournisseurs de logiciels de RF ou ceux qui contrôlent les bases de données d'empreintes faciales que consultent les services de police.

En l'absence de dispositions légales de nature à rendre responsables les tierces parties en qualités de sous-traitants (contrairement au RGPD)[1], le contrat conclu entre ces entreprises privées et les services de police devrait contenir un certain nombre de mentions et obligations pour imposer le respect des législations et un niveau élevé de protection des renseignements personnels.

Il faudrait également permettre certaines vérifications en période précontractuelle avant tout engagement contractuel. En particulier, des audits préalables des systèmes devraient être mis en œuvre. Devrait être également précisées les méthodes utilisées pour entraîner les systèmes, ainsi que les données d'entraînement utilisées. Les scores de similitude (taux d'erreur) devraient être donnés, ainsi que les procédures mises en œuvre pour contrôler l'évolution des systèmes (itération).

6. Anticipez-vous des conséquences négatives découlant des recommandations présentées dans ce document d'orientation et, si c'est le cas, lesquelles?

Le principal risque que nous voyons serait que ces recommandations soient trop complexes et pas assez opérationnelles et, partant, ignorées.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)(Texte présentant de l'intérêt pour l'EEE), <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR>.

OBSERVATIONS SUR LE CADRE JURIDIQUE ET DE POLITIQUE APPLICABLE AU RECOURS À LA RF PAR LES SERVICES DE POLICE

7. Le recours à la RF par les services de police est-il encadré de façon appropriée au Canada par les lois existantes?

Nous considérons que le recours à la reconnaissance faciale par les services de police n'est pas suffisamment encadré au Canada, tout comme de nombreux autres États.

Nous renvoyons à ce sujet à notre rapport sur « le Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada : éléments de comparaison avec les États-Unis et l'Europe » publié par l'OBVIA [Castets-Renard 2020][2]. Voir Aussi Woodrow Hartzog, Professeur à la Faculté de droit de la Northeastern University à Boston, pour qui la reconnaissance faciale représente « le parfait outil pour l'oppression » [Hartzog 2018][3], validant ainsi les analyses inquiètes exprimées sur le plan de la sociologie et dans le champ des « Surveillance Studies » par David Lyon [Lyon 1994[4] et 2009[5] ; Lyon & Bennet 2008][6].

Si ce n'est pas le cas, quelles sont vos préoccupations quant à la façon dont l'utilisation de la RF par les services de police est encadrée aujourd'hui et quelles modifications devraient être apportées au cadre juridique actuel ?

Nos principales préoccupations sont de plusieurs ordres.

Tout d'abord, il faut noter que la plupart des technologies policières sont conçues par des entreprises privées et directement proposées aux services de police à différents niveaux (fédéral, provincial, territorial, municipal). Or, ces derniers n'ont pas nécessairement les compétences en interne pour comprendre et éprouver les systèmes qui sont proposés. Ces systèmes restent largement opaques, les données d'entraînement utilisés méconnus. Les services de police sont les utilisateurs et non les concepteurs de ces systèmes mais ne sont pas suffisamment bien informés de leurs caractéristiques et ne peuvent pas les maîtriser. Une certaine dépendance envers ces entreprises privées est alors constatable.

Les partenariats public-privé qui s'établissent ici entraînent donc des relations déséquilibrées au détriment de la police. Ce déséquilibre est accentué par des politiques commerciales « agressives » de ces entreprises technologiques qui proposent souvent leur produit « gratuitement » à l'essai et laissent ainsi croire aux services de police qu'il n'y a « rien à perdre à essayer ». Les services de police ne sont pas le plus souvent informés des risques

---

[2] <https://observatoire-ia.ulaval.ca/rapport-reconnaissance-faciale/>.

[3] Facial Recognition Is the Perfect Tool for Oppression, Medium (2018), <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

[4] The Electronic Eye: The Rise of Surveillance Society (1994).

[5] Identifying Citizens: ID Cards as Surveillance (2009).

[6] Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (2008).

sociaux et éthiques qui peuvent découler de leur usage ni des moyens qu'il faudrait mettre en œuvre pour les minimiser. En outre, les relations contractuelles sont déséquilibrées en raison d'une forte asymétrie d'information sur le fonctionnement concret de la technologie, sur ses possibilités et surtout ses limites.

De façon générale, on sait que les partenariats public-privé portent souvent atteinte à la protection des renseignements personnels et de la vie privée. Cela est d'autant plus vrai lorsque les entreprises privées sont situées à l'étranger, en particulier aux États-Unis, où la protection des renseignements personnels sera plus difficile à garantir et qu'il n'existe pas de moyens très efficaces pour les contraindre à respecter le droit canadien.

Ensuite, il faut noter un manque de transparence de l'utilisation des technologies par la police. Les lieux et motifs de déploiement sont méconnus par la population. Or, compte tenu des forts enjeux sociaux pour la société et les droits fondamentaux des individus, une plus grande transparence devrait être mise en œuvre. Le public serait certainement plus enclin à accepter l'usage de cette technologie si les avantages pour la sécurité lui sont présentés.

Plus globalement, la balance coûts/avantages devrait faire l'objet d'un débat public au sein des parlements et ne pas être laissée à la seule appréciation des chefs et services de police. Au final, la principale préoccupation tient au fait que le recours par la police à la reconnaissance faciale n'étant pas encadrée, elle ne peut par hypothèse faire l'objet de limitations et peut se déployer « à tout va ». Or, on le sait, cette technologie génère de nombreux risques sociaux et est susceptible de porter atteinte à plusieurs droits fondamentaux (vie privée, égalité et non-discrimination, présomption d'innocence, liberté de manifestation…), protégés par la Charte canadienne des droits et libertés, la Charte québécois des droits de la personne et autres lois provinciale sur les droits de la personne.

Si le recours à cette technologie peut trouver une justification sociale dans certains cas et dans le cadre de certaines infractions, elle doit quoi qu'il en soit faire l'objet de conditions et d'un cadre légalement défini dont le respect serait garanti par des sanctions réelles. Les risques sociaux sont trop élevés pour laisser la décision de recourir à la reconnaissance faciale aux seuls corps de police. Ces derniers bénéficieraient d'ailleurs d'un cadre clair dans lequel ils pourraient être autorisés à agir et qui garantirait la fiabilité des résultats, ainsi que la sécurité juridique des procédures mises en œuvre.

Vaudrait-il mieux que ces modifications soient abordées dans un cadre règlementaire distinct qui porte précisément sur l'utilisation de la RF ou dans le contexte de la réforme des lois sur la protection des renseignements personnels (application générale) ?

Il nous semble que si des améliorations pourraient être apportées dans les lois sur la protection des renseignements personnels, ce support législatif serait insuffisant. En effet, la reconnaissance faciale combine données biométriques et système d'IA de reconnaissance d'images, aussi convient-il de considérer les deux.

D'une part, la reconnaissance faciale suppose l'utilisation massive de données personnelles biométriques qui, ailleurs dans l'Union européenne (RGPD, art. 9), sont considérées comme des données sensibles qui ne peuvent en principe faire l'objet d'un traitement, sauf

exceptions limitativement énumérées. Il pourrait y avoir ici une première amélioration législative dans l'encadrement des données sensibles, dont les données génétiques et biométriques. Il est pertinent d'utiliser ces catégories largement plutôt que d'envisager les technologies séparément, au risque de devoir légiférer trop souvent.

Également, le régime de protection des renseignements personnels pourrait être amélioré s'agissant de la chaîne d'intervenants dans le traitement des données personnelles. Les systèmes d'IA proposés par les entreprises privées nécessitent le plus souvent un échange et partage constant des données biométriques entre les services de police et les entreprises privées qui proposent un service de reconnaissance évolutif plutôt que l'exécution d'un contrat en « un trait de temps ». Ce contrat de prestation de services suppose le traitement de renseignements personnels, lesquels sont de fait souvent envoyés aux États-Unis. Dans ces conditions, même si on estime que le droit canadien est applicable, il paraît très difficile de contrôler son respect par ces entreprises en l'état actuel du droit. L'affaire Clearview AI illustre cette problématique. Sur ce point, il pourrait être utile de réformer les législations sur la protection des renseignements personnels en rendant responsables ces entreprises que l'on pourrait qualifier de sous-traitantes sur le modèle du RGPD. Cela ne remettrait pas en cause la responsabilité des polices qui pourraient en outre être explicitement tenues de bien choisir leurs sous-traitants et de vérifier leur capacité à respecter le droit canadien, notamment l'obligation de collecte licite de renseignements personnels, comme il a été défendu par les autorités de protection des renseignements personnels du Canada dans l'affaire Clearview AI. Une obligation explicite en ce sens devrait être ajoutée dans les législations du secteur public.

Enfin, l'encadrement de l'utilisation de la RF par les services de police au Canada ne porte pas seulement sur les vertus ou les défauts de lois de protection des renseignements personnels. Il convient surtout de considérer avant tout le type d'autorisation judiciaire préalable que ce mode de surveillance exigerait pour respecter l'article 8 de la Charte. Il existe des mandats spécifiques pour différentes techniques d'enquête comme l'interception des communications privés, l'utilisation de balises GPS et les analyses ADN. Les modalités d'octroi de ces mandats sont prévues dans le Code criminel. En l'état actuel du droit, il faut s'en remettre à un mandat général et moins exigeant pour autoriser le recours à la reconnaissance faciale, prévu à l'article 487,17 du Code criminel. Il faudrait créer un régime spécial par l'adoption d'une loi qui ajouterait le besoin d'un mandat spécial dans la partie 6 du Code criminel.

D'autre part, il nous semble indispensable de considérer la spécificité et la dangerosité de la reconnaissance faciale comme système d'IA. Plusieurs options législatives sont alors envisageables.

Une première façon de faire pourrait être d'encadrer uniquement cette technologie dans le cadre d'un usage policier, comme on l'a vu apparaître dans certaines villes des États-Unis[7].

[7] Voir par exemple : New-York City Council, Int 0487-2018 du 15 juillet 2020, <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0>.

Cette approche serait très sectorielle et donc limitée mais viserait le champ matériel de ce document d'orientation.

Une autre façon d'envisager la loi serait de chercher à encadrer l'ensemble des technologies policières utilisées à ce jour et non pas seulement la reconnaissance faciale. Pourraient être ainsi visées notamment : les logiciels d'analyses prédictives qui « anticipent » la survenance de risques d'infractions ; les logiciels d'évaluation du score de dangerosité des individus ; les systèmes de lecture automatique de plaques d'immatriculation ; les caméras corporelles portées par les policiers. Il apparaît en effet que, de façon générale, le public n'est pas informé des différentes technologies existantes et de ce qui est effectivement mis en œuvre, dans quels lieux, pour quels motifs et dans quelles circonstances. Ce manque de transparence n'est pas favorable à la confiance entre le public et la police, pourtant indispensable. Elle n'encourage pas non plus l'acceptabilité sociale de la technologie, alors même que l'IA peut naturellement présenter des avantages pour la sécurité du public.

Une troisième façon de faire serait d'encadrer l'utilisation des systèmes d'IA de façon plus globale, suivant une législation transversale dite « omnibus », à l'instar de la proposition de la Commission européenne sur l'intelligence artificielle publiée le 21 avril 2021[8]. La Commission européenne choisit de règlementer la mise sur le marché des systèmes d'IA, lesquels sont définis très largement à l'annexe I de la proposition, par souci de ne pas entrer dans les détails techniques et de garantir une neutralité technologique. Notons par ailleurs que l'approche transversale de la proposition de la Commission européenne n'empêche pas la mise en œuvre de règles spécifiques plus sectorielles par domaines ou types de technologies. Une double dynamique transversale et sectorielle irrigue ainsi ce texte. On constate alors que la reconnaissance faciale est spécifiquement règlementée au titre des systèmes interdits en raison de risques inacceptables (article 5) et au titre des systèmes à hauts risques (annexe III) selon les contextes de sa mise en œuvre. L'hypothèse d'interdiction concerne l'usage de la reconnaissance faciale en temps réel dans des espaces publics à des fins répressives. Cette interdiction est toutefois limitée par trois catégories d'exceptions dont la dernière est particulièrement large (32 infractions visées dont des infractions économiques comme des fraudes). Ces exceptions remettent ainsi amplement en cause le principe. Elles sont toutefois assorties d'un régime juridique présentant des garanties procédurales par un contrôle d'une autorité judiciaire ou d'une autorité administrative indépendante, ainsi que des limites dans le temps et dans l'espace. On peut donc dire finalement que même si l'utilisation de la reconnaissance faciale par la police est autorisée dans certains cas, elle doit être mise en œuvre dans les limites d'un cadre légal. Cette proposition de texte parvient finalement à encadrer à la fois la mise sur le marché de l'IA en général, d'une part, et la reconnaissance faciale à des fins répressives plus spécifiquement, d'autre part.

Au final, si la troisième voie est particulièrement ambitieuse et sans doute difficile à atteindre dans le cadre du système fédéral canadien, les deux autres voies devraient retenir l'attention du législateur canadien et des législateurs provinciaux et territoriaux mais aussi des municipalités. Même si la première voie était retenue en ne visant que la reconnaissance

[8] <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0020.02/DOC_1&format=PDF>.

faciale, ce serait déjà un progrès en soi, d'autant plus que cette technologie est certainement la plus dangereuse. Quelle que soit l'option législative retenue, l'encadrement de la reconnaissance faciale par les services de police est un minimum à garantir aux citoyens.

8. Quelles mesures de protection devraient être offertes aux personnes dont les renseignements biométriques sont versés dans une base de données contenant des empreintes faciales?

Il nous semble qu'il faudrait d'abord s'appuyer sur les législations sur la protection des renseignements personnels en mettant notamment l'accent sur trois dimensions importantes : la limitation de la durée de conservation, l'exactitude et la mise à jour des données, la sécurité des données.

La limitation de la durée de conservation suppose la mise en œuvre d'un droit à l'effacement à l'expiration d'un délai qui devrait être court et clairement fixé par la loi. Plus généralement, il ne devrait pas y avoir de conservation possible des données s'il n'y a pas de motif de surveillance de la personne concernée dans le cadre d'une procédure pénale. Autrement dit, la conservation des données devrait être justifiée dans le cadre d'une procédure pénale pour une surveillance ciblée. Le respect de ce droit à l'effacement suppose la mise en œuvre d'une obligation stricte à la charge des personnes qui détiennent les données. Cela pourrait en particulier se traduire par la mise en œuvre d'un système de purge automatique des données.

Également, l'obligation de collecter et conserver des données exactes et à jour devrait s'appliquer avec rigueur pour éviter les risques d'erreur et de mauvaise identification des personnes. L'obligation d'actualiser les données suppose aussi la mise en œuvre de procédures automatiques de vérification et rectification en cas d'erreur.

Quant à la sécurité des données personnelles, elle est particulièrement nécessaire s'agissant de données biométriques par nature sensibles. Des règles strictes de conservation et de respect des bonnes pratiques de cybersécurité doivent s'appliquer au sein des polices. Si on peut s'attendre à ce que cela soit le cas au niveau de la police fédérale, il faut sans doute interroger aussi les polices provinciales, territoriales et surtout municipales et veiller à ce qu'elles soient toutes dotées des moyens nécessaires pour garantir cette sécurité. Il faut aussi interroger les conditions de circulation de ces données entre les polices et/ou la centralisation de l'information dans une ou plusieurs bases de données.

Par ailleurs, au-delà de la législation sur la protection des renseignements personnels, il convient aussi d'interroger les systèmes de reconnaissance faciale en eux-mêmes en mettant en place des mesures qui permettent d'éviter ou de limiter les risques d'erreurs et les discriminations dans l'utilisation de ces renseignements. Pour ce faire, les données d'entraînement des modèles, de validation et de test devraient répondre à certaines exigences et respecter des bonnes pratiques en matière de gouvernance et gestion des données. Ces pratiques portent sur les choix de conception pertinents, la collecte de données, les opérations de traitement pour la préparation des données (annotation, étiquetage, nettoyage, enrichissement et agrégation), une évaluation préalable de la

disponibilité, de la quantité et de l'adéquation des jeux de données nécessaires, un examen des éventuels biais, la détection d'éventuelles lacunes ou déficiences dans les données.

De façon générale, le jeu de données d'entraînement, de validation et de test devrait être pertinent, représentatif, exempts d'erreurs et complets. La difficulté est que les systèmes et les jeux de données peuvent être mis en œuvre par les services de police qui peuvent être conduits à créer leurs propres outils de reconnaissance faciale. Mais, comme vu auparavant, ces outils peuvent être aussi créés par des entreprises privées et les services de police sont alors de simples utilisateurs et non les concepteurs. Quoi qu'il en soit, si on veut que de telles mesures aient un sens et une efficacité, il convient de les appliquer aussi bien aux entreprises qu'aux services de police. Elles devraient ainsi viser tous les concepteurs d'outils de reconnaissance faciale utilisés par la police, quels qu'ils soient. Le respect de ces obligations devrait être garanti par l'obligation d'établir une documentation technique, à l'instar de ce que prévoit l'annexe IV de la proposition de règlement sur l'IA de la Commission européenne.

9. L'utilisation que font les services de police de la RF, y compris la collecte des empreintes faciales, devrait-elle se limiter à un ensemble déterminé de fins (comme pour les crimes graves ou pour des raisons humanitaires, par exemple dans le cas de personnes disparues)?

Il nous semble en effet qu'il faudrait limiter l'utilisation policière de la reconnaissance faciale à certaines infractions qui devraient être limitativement énumérés. Il conviendrait aussi qu'il s'agisse d'infractions graves et que leur choix soit transparent et justifié. Il faut noter que la proposition de règlement de la Commission européenne sur l'IA interdit l'utilisation de la reconnaissance faciale en temps réel dans des espaces publics sous réserve d'exceptions (article 5 de la proposition). Or, les infractions autorisant par exception la reconnaissance faciale sont nombreuses (32 infractions) et ne paraissent pas justifiées par la gravité de l'infraction (ex. fraude). Sur ce point, la proposition n'est pas un exemple à suivre selon nous.

Les services de police devraient-ils être en mesure d'utiliser ou de conserver des empreintes faciales autres que celles des personnes qui ont été arrêtées ou condamnées?

La conservation des empreintes et bases de données devraient en effet se limiter aux personnes arrêtées ou condamnées (fichier des antécédents judiciaires). Il convient en particulier de ne pas conserver des informations des personnes se trouvant sur des lieux où la reconnaissance faciale a été activée, dès lors que ces personnes n'auraient finalement pas de lien avec une infraction. En particulier, les données des personnes relaxées ne devraient pas être gardées. Ne devraient pas non plus être conservées les données de simples témoins. Par ailleurs, s'il s'avère qu'une infraction est requalifiée et qu'elle sort alors des cas listés autorisant les services de police à utiliser la reconnaissance faciale, il faudrait également veiller à ne pas conserver les données. Il s'agit là de quelques exemples illustrant le fait qu'il convient de limiter les personnes et les cas de collecte des empreintes faciales.

Existe-t-il des situations dans lesquelles les services de police ne devraient jamais être autorisés à recourir à la RF, ou des applications particulières de la RF qui devraient être interdites (c.-à-d. des « zones interdites » telle que le prélèvement systématique des images sur Internet)? Des règles spéciales (ou une interdiction) devraient-elles encadrer l'application de la RF aux jeunes?

S'agissant des situations d'interdictions par principe, il semble difficile d'énumérer des cas d'interdiction totale en soi. Les impératifs de sécurité publique sont forts et le droit à la sécurité est aussi un droit fondamental des individus. En revanche, il serait possible de prévoir des situations dans lesquelles l'usage de la reconnaissance faciale serait inacceptable comme un usage systématique et massif dans l'espace public en dehors de tout contexte d'une dangerosité particulière. Il s'agirait là d'une surveillance de masse qui ne peut être acceptée par principe sans énumérer des infractions ou circonstances spécifiques. Le risque pour la démocratie est ici très élevé.

De même, l'utilisation de la reconnaissance faciale dans le cadre de rassemblements et manifestations d'opinions dans la rue est une hypothèse à considérer avec attention. Le risque démocratique est très élevé ici aussi, si on envisage les opposants politiques au gouvernement en place qui pourraient se trouver surveillés. De nombreux exemples dans le monde, comme au Mexique, montrent que ce risque majeur est malheureusement réel, y compris dans des sociétés considérées comme démocratiques.

Notons par ailleurs que des circonstances dans lesquelles la reconnaissance faciale serait associée à d'autres technologies, comme les drones ou les caméras corporelles, ne seraient pas acceptables. On peut d'ailleurs noter que plusieurs lois adoptées aux États-Unis vont en ce sens[9].

S'agissant des applications particulières, la reconnaissance faciale reposant sur une collecte illicite d'images ne devrait pas être autorisée. De façon générale, dès lors que la législation sur la protection des renseignements personnels n'est pas respectée, la mise en œuvre des données obtenues illicitement au sein d'une quelconque technologie d'IA ne saurait être licite. L'opération de traitement des données dans le contexte de la technologie d'IA ne peut permettre de « blanchir » l'activité illicite à l'origine. Un principe général devrait ainsi être posé, selon lequel l'usage d'une technologie d'IA ne saurait être licite dès lors que les données (en particulier les données personnelles mais cela peut valoir aussi pour d'autres données protégées) ont été collectées de façon illicite. Ce point rejoint la position des autorités de protection des renseignements personnelles dans l'affaire Clearview AI.

Enfin, nous sommes aussi favorables à ce que l'usage de la reconnaissance faciale ne s'appliquent pas aux mineurs, non seulement pour protéger ce public particulièrement vulnérable mais aussi en raison d'un fort risque d'erreur les concernant, dès lors que leurs visages évoluent encore fortement.

---

[9] Oregon - HB 2571 du 5 mai 2015. Californie - AB-1215 Law enforcement: facial recognition and other biometric surveillance du 8 octobre 2019. Etat de New-York - A4030, Assembly Bill on Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof.

10. Existe-t-il d'autres enjeux importants en matière de politiques sur lesquels il y aurait lieu de se pencher en rapport avec l'utilisation que font les services de police de la RF? Sont notamment visés de nouveaux enjeux à caractère juridique, éthique ou social entourant le développement et la mise en œuvre de bases de données d'empreintes faciales par les services de police. Si c'est le cas, quels sont ces enjeux et comment recommanderiez-vous que l'on intervienne à leur égard?

Nous tenons à souligner l'enjeu social fondamental que constituent les risques d'erreur et de biais, discrimination et exclusion de certaines communautés. Sans oublier le fait d'une transformation de l'espace social qui peut devenir transparent. Comme l'affirme Thierry Menissier (2019)[10], les risques engendrés par un déploiement non contrôlé sur la vie sociale mettent en danger la vie privée en violant notamment l'anonymat auquel chacun a droit dans une démocratie.

L'enjeu juridique : le risque d'erreur porte atteinte à la présomption d'innocence. Si cet enjeu dépasse bien sûr l'atteinte au droit fondamental à la vie privée, c'est la collecte de données personnelles biométriques et la fausse inférence au moment de l'identification qui permet de porter atteinte à ce droit. Le risque de biais porte à l'évidence atteinte au principe d'égalité et à la non-discrimination.

On constate ainsi souvent que l'atteinte à la vie privée s'accompagne de l'atteinte à d'autres droits humains. Une analyse des risques envers les droits humains est indispensable et peut se réaliser au travers de l'étude de risques pour la vie privée, telle que présentée dans ce document d'orientation.

Il conviendrait en outre de considérer la question de la procédure et en particulier de la preuve des atteintes à ces droits humains en cas d'utilisation de la reconnaissance faciale. Si la preuve de l'atteinte à la vie privée ne semble pas causer de grosses difficultés, la preuve d'une discrimination algorithmique ou d'une erreur est difficile à rapporter. Il conviendrait alors de réfléchir aux mécanismes de preuve et d'envisager une inversion de la charge de la preuve qui pèserait sur les concepteurs et /ou utilisateurs de ces outils et non sur les personnes à qui les outils d'IA sont appliqués. Il reviendrait ainsi aux services de police de prouver que le système de reconnaissance faciale n'est pas discriminant et ne commet pas d'erreurs ou pour le moins parvient à un niveau « acceptable » en minimisant les risques. La mise en œuvre de bonnes pratiques dans le système de gestion des risques et la gouvernance des données du système d'IA pourrait être un moyen privilégié d'apporter des garanties. La mise en œuvre d'une documentation technique dont les exigences seraient bien précisées permettrait de rapporter cette preuve.

L'enjeu éthique : Ce dispositif biométrique qu'est la reconnaissance faciale soulève un enjeu éthique dès le début : elle capte des données issues du corps humain sans contact ni

[10] Les dispositifs de reconnaissance faciale : une réalité socio-technique en développement, un enjeu pour les libertés publiques et privées, un défi pour l'éthique de l'IA, <https://halshs.archives-ouvertes.fr/halshs-02395401/document>.

consentement préalable. Ainsi l'éthique peut contribuer à l'évaluation des technologies de l'IA étant donné le contexte de perte de repère traditionnel sous l'émergence de ce dispositif.

Intégrer l'éthique en matière de RF a pour objectif de réfléchir aux valeurs qui influencent le choix des interventions tout en ayant pour but d'établir la légitimité et l'acceptabilité sociale. Pour ce faire, il nous apparait important de se doter d'outils éthiques pour reconnaître les valeurs qui sont en jeu et en saisir la signification. Actualiser cette composante dans les choix qui seront faits peut jouer un rôle important dans la préservation et le renforcement de la confiance des citoyens et éviter de glisser dans l'ère du contrôle absolu sans sous-estimer le risque de mise en œuvre d'une société de surveillance intégrale et invisible.

Il nous apparait essentiel de proposer un référentiel de valeurs visant à éclairer les interventions en matière de sécurité publique et mieux soutenir la réflexion des professionnels afin qu'ils puissent bien saisir les risques, les conséquences et les valeurs qui sont menacées. Un tel débat, permet d'établir au nom de quelle valeur on va agir et ainsi voir plus clairement la société qui peut aujourd'hui être désirable. Proposer un processus d'examen éthique pour les actions à prendre au regard de la RF en matière de sécurité publique aiderait à la compréhension de ces actions de même qu'aux responsabilités qui en découlent : « *…la visée de l'éthique est de conduire à une décision réfléchie et délibérée plutôt que mécanique, après avoir interrogé les automatismes, après avoir sondé ses propres assis et après avoir pris en considération le sens partagé. […] cette décision doit aussi être justifiable, l'individu devant être en mesure de répondre de sa décision aux autres.* » (Boisvert et al., 2003)[11]. Ainsi, un référentiel de valeurs fournit une ressource précieuse pour un jugement éthique approfondi.

La prise en compte des enjeux juridiques et éthiques est source de confiance et acceptabilité sociale nécessaires au déploiement de toute technologie.

[11] Y. Boisvert, M. Jutras, G. Legault, H. Marchildon & L. Côté (2003). Petit manuel d'éthique appliquée à la gestion publique. Collection Éthique publique. Liber, Montréal.